DOCUMENT RESUME

ED 275 303 IR 012 363

AUTHOR Kirby, Michael D.
TITLE The Ten Information Commandments.
PUB DATE Jun 86
NOTE 5p.; Excerpts from the Keynote Address to the National Forum on Access to Information and Privacy (Ottawa, Canada, March 6, 1986).
PUB TYPE Viewpoints (120) -- Speeches/Conference Papers (150)
JOURNAL CIT Transnational Data and Communications Report; v9 n6 p19-22 Jun 1986

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS *Access to Information; Communications; Foreign Countries; Futures (of Society); *Information Dissemination; *Information Technology; Information Utilization; *Legal Problems; *Privacy; Science and Society; *Technological Advancement

ABSTRACT

In response to fears that current institutions and laws may not adapt to rapid technological change with the necessary alacrity, a justice of the Supreme Court of New South Wales presents and briefly discusses ten information commandmants, summarized as follows: (1) contemporary technological developments endanger human rights and civil liberties and require responses from society, including the legal system; (2) the common law system is insufficient to provide adequate responses to the challenges of technology--legislation is needed; (3) in some cases the technology itself demands or even produces legal reform; (4) the people are not always the best judges of their own interests--informed observers have a duty to identify dangers to freedom; (5) the costs of the right to information must be counted, but so must the intangible benefits; (6) information laws must be developed flexibly because of changing technology and the rapidly changing perceptions of the problems; (7) information rights must extend from the public sector to the private sector; (8) information technology presents international issues that require international solutions; (9) legal responses to information rights must attend to real problems and not content themselves with myths and mere symbols; and (10) democratic values must be preserved. (KM)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED275303

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
☒ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY
T.G. Donovan
TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

The Ten Information Commandments

by Michael D Kirby
President, Court of Appeal,
Supreme Court of New South Wales, Sydney

Kirby

The other day, as light relief to Archbold's *Criminal Pleadings* and Dicey's *Law of the Constitution*, I was reading the writings of Marx. Not, mind you, Karl; but Garry Marx, a New York academic. The thesis which Marx propounded provides the theme song for this National Forum. Asserting that popular culture, and hit tunes, can sometimes convey, even subliminally, important political and social messages, Marx took as an illustration the hit song of the pop group The Police. Hidden away in the words, he said, was a timely warning to the younger generation of the dangers of the new information technology. The song is 'Every Breath You Take'. Here is Marx's analysis:

'Every breath you take [breath analyzer],
Every move you make [motion detector],
Every bond you break [polygraph-lie detector],
Every step you take [electronic anklet],
Every single day [continuous monitoring],
Every word you say [bugs, wire taps, mikes],
Every night you stay [light amplifier],
Every vow you break [voice stress analysis],
Every claim you stake [computer matching],
Every smile you fake [brain wave analysis],
I'll be watching you [video surveillance].'

Marx's thesis is as frightening as it is simple. We stand at the brink of remarkable developments in the thriving new technology of informatics both in the public and private sectors. Some of the developments are regulated by current law. Many of them are outside. Computers may match the hundreds of profiles built up on all of us. In the last decade, there has been a massive increase in the ability to collect and process intrusive information about all of us which, but a few years ago, would have been regarded as utterly private and totally inaccessible – even to the most powerful government official or corporate enterprise.* Satellites can spot a car or person from 30,000 feet up. They have been used for surveillance of drug traffickers. Light amplifiers, developed for the Vietnam war, can be used with a variety of cameras and binoculars to intrude into the private moment. National security agencies monitor hundreds of telephones. The Hong Kong government is testing an electronic system for monitoring where, when and how fast a car is driven. A small radio receiver in the car picks up low frequency signals from wire loops set into the street. It then transmits back to a central authority the car's identification number. The system was proposed as an efficient means for the relatively innocent task of checking the payment of road tax in the congested traffic areas of Victoria Island. But what a boon it provides, or would provide for continuous monitoring and surveillance.

This is not alarmist talk. The features of the new information technology which endanger the value of individual privacy are now well known. According to Marx, the dangers derive from the following features of the technology in particular:

- it transcends distance, darkness and physical barriers;
- it transcends time, because of the capacity to collect and store massive amounts of data which can be retrieved whenever needed;
- it is capital- rather than labor-intensive, because it is no longer necessary to have human intervention. The computer can analyze all;
- it is universal in its application, decentralized and triggers self-activating policing;
- it has low visibility or even total invisibility;
- it grows ever more extensive and covers larger areas of life, ever more deeply.

These are trite statements about a pervasive technology which is overwhelmingly beneficial in its potential to release mankind from the millstones of routine and mindless drudgery.

The past decade or so has seen important legislative responses to informatics in all the advanced English-speaking

* Garry Marx, 'I'll be Watching You' in *Dissent*, Winter 1985.

IR 013363

democracies. Much more must certainly be done. As a contribution to the public policy debate, I have decided, with due modesty, to propound the ten information commandments.

The commandments

1. Contemporary technological developments endanger human rights and civil liberties and require responses from society – including the legal system.

This first 'commandment' states the obvious. It is not confined to informatics. The most remarkable feature of the late 20th century is the coincidence, at one moment of history, of three important technological developments. I refer to nuclear fission, biotechnology and informatics. Each of these developments has implications for human rights and civic freedoms. Information technology presents problems, some of which have been identified already by Garry Marx. We need a Luther of jurisprudence to lead us to the legal solutions, and political leaders of wisdom to guide our communities thoughtfully to the responses that preserve life and freedom.

2. The fertile common law system, even as enhanced in some countries by constitutional rights, is insufficient to provide adequate responses to the challenges of technology. Legislation is needed.

There are some people who say that the common law, developed by the judges, will be adequate to defend our liberties – in the future as it has in the past. No doubt there is a role for the common law. It must surely respond to technological change. Benjamin Cardozo once said that the law, like the traveler, must prepare for the morrow. In the United States, with the famous language of the Bill of Rights, and in Canada with the Charter, a scope is offered to the judiciary to enhance the creative element which has always existed in the common law. But even in such countries, and even more so in countries such as my own, without such a catalyst for judicial creativity in the protection of rights in the modern era, more will be needed.

3. In some cases the technology itself demands or even produces legal reform.

This third rule refers to the tendency of modern technology to undermine current law or to render it irrelevant or ineffective. I refer to the way in which the photocopier undermines excessive secrecy. Doubtless this is why photocopiers are kept onder lock and key in the Soviet Union. The technology of photographic reproduction and online linkages reduces the capacity to keep things secret. The selfsame technology that presents the problems of privacy promotes the flow of information that tends to enhance accountability both in the public and private sectors. Information technology with its international applications reduces, by transborder data flow, the effective operation of the sovereign laws of domestic jurisdiction.

4. The people are not always the best judges of their own interests. Informed observers have a duty to identify dangers to freedom.

This Fourth Commandment teaches that we *should* care. And that it is the responsibility of politicians, and those who advise them, to work, even in the face of popular indifference or opposition, for the preservation of hard-won freedoms. For once they are lost they are rarely regained.

5. The costs of information right must be counted. But so must the intangible benefits.

In the jargon of the economist it is important for lawyers who talk of liberty and freedom to take into account the incremental costs involved in the externalities to decision making. The protection of freedom and the assurance of fairness have a cost. The combination of talk about cost of the provision of information rights, the inevitable concern by politicians about skeletons they would rather leave in the computer cupboard, and the hankering of not a few public servants for a return to the 'good old days', all present the danger of the Information Counter Reformation. It is a danger which supporters of information rights must repell.

Against the cost of providing information that people want to know must be considered the cost of official government information services that nowadays pour out thinly disguised propaganda, repeated through media handouts, concerning what the government *wants* people to know. The former may be a healthy corrective, on occasion, to the latter.

6. Information laws must be developed flexibly because of changing technology and the rapidly changing perceptions of the problems.

Not to devise and implement privacy laws, in the inadequacy of the common law and current legislation, is to make a decision. It is to stand quietly by whilst the technology itself erodes hitherto valued rights. But the counterpart of this principle is that inflexible laws can outlive the understanding of the problem they have been introduced to solve. This is why Spiros Simitis has said that data protection laws are now at a 'turning point'. An illustration of this truism can be given. Many of the laws already put in place rely heavily on the right of individual access as a means of protecting individual privacy rights. But the effective utilization of this most beneficial right depends upon large assumptions. It depends upon knowledge by the individual that there is something to be concerned about. If there is no notification that you are in the system, decisions may be made, vital to your life. And yet you may be blissfully ignorant. Similarly, the right of access makes large assumptions about individual initiative and enthusiasm. Realism might well raise different considerations. Apathy, resignation or a feeling of powerlessness may necessitate other solutions, if true data protection is to be afforded – beyond the powerful and articulate who exert their rights. There is a tendency in our kind of society to slip into legislative mythology. It is an easy myth to believe that accountability is provided

by a right of access and that information rights are thereby protected. In fact, such facilities should be seen as the start of a long journey – not arrival in the Promised Land.

7. *Information rights must extend from the public sector (where they have been developed) to the private sector.*

So far, comprehensive information laws have concentrated on the public sector. This is natural for it is in that sector that critical information affecting all citizens exists. But increasingly important in our lives, and often insusceptible to national control, are large corporations – including transnational corporations. People in the private sector tend to be foremost in asserting the right of accountability by public officials and access to public data. But the selfsame principle has relevance to the private sector as well. Its full relevance is yet to be worked out. Of course, there is already much accountability by the private sector – including in the market. But information rights concern individual power. And power exerted in relation to the corporate state may be equally applicable in relation to dealings with private enterprise. Voluntary guidelines, such as compliance with the OECD privacy principles, may provide a starting point. But it is scarcely likely that this will be adequate in the long term.

8. *Information technology presents international issues that require international solutions.*

The need for transborder solutions to information rights is self-evident in federations such as Australia, Canada and the United States. But there is a wider international stage. The technology itself is universal. The problems presented necessarily transcend state borders. The OECD Guidelines were developed in the hope of stimulating consistency in legislative and administrative approaches to information rights in the context of privacy. Now, other international agencies are endeavoring to develop rules which can facilitate common approaches. UNESCO has just embarked on a major informatics program. The Intergovernmental Bureau for Informatics (IBI) in Rome has established a commission to promote a dialogue on data law and policy between the advanced countries of the OECD and the developing world. The technology must interface. Gross inefficiency will result if legal regulations are enacted which are incompatible and yet must be complied with by transborder flows of data. Data havens may destroy the effectiveness of information rights. The three technological developments of our time – nuclear fission, biotechnology and informatics – require of us that we should lift our sights from parochial and purely nationalistic approaches to the law. Until now, law has been very much jurisdiction-bound. International technology imposes on us the need for international approaches to legal regulations. That is why fora such as this have a special utility. We in the developed world must become more conscious of the needs and concerns of those less rich. They follow the caravan of the information economy.

9. *Legal responses to information rights must attend to real problems and not content themselves with myths and mere symbols.*

This principle has already been foreshadowed. The easy thing for lawmakers to do is to establish a bureaucracy with attractive titles, set up with a fanfare announcing that information is free and privacy is guaranteed. What is important is the fine print. It has always seemed to me that the value of the OECD Guidelines lay chiefly in the formulation of a short list of relatively simple principles for information practices. If these became well known and generally accepted as a bible of fair information practices, much would be achieved. Sanctions and advisory mechanisms are needed to deal with the problems that arise. But most people at the work face simply require a series of simple rules, ultimately backed up by the law. The simpler the rules are kept and the fewer in number, the more likely it is that fair practices will result. In the field of FOI, rights of access will not promote effective accountability unless they are reinforced by community rights of access to the public media. The concentration of the media in few hands may undermine the effectiveness of official information laws because they prevent vital information flowing through to the community at large. Thus it is the reality of information rights that we should be concerned with, not the mythology. Laws which talk of 'the consent of the data subject' sound fine. But to an unemployed pensioner seeking a social security benefit, or a hospital patient seeking treatment, or an employee seeking information which does not result in dismissal or destroy advancement prospects, it may sometimes be necessary to go beyond reliance on the courageous individual. Information laws which depend exclusively on individual motivation for enforcement are much better than nothing. They are a step in the right direction. But they fall a long way short of providing effective protections against all the implications of the new technology.

10. *Democratic values must be preserved, and it is at least questionable whether our democratic institutions can adequately respond to the challenges of technology.*

This brings me to my last 'commandment'. I approach my conclusion on a sombre note. Those who look at the history of parliamentary democracies this century, at least in our countries, may be generally optimistic about the future. Despite many challenges the institutions have survived. The alternative systems are infinitely less flexible and uniformly more oppressive. But the problem for parliamentary institutions, posed by rapid technological change, is that of keeping pace. If nothing is done, a decision is made. Yet the very technicality of the changes makes it difficult for the lay politician (and indeed those advising him or her) to comprehend all the ramifications. Furthermore, many of the changes are highly controversial, as debates about the privacy of children against their parents and about biotechnological experiments clearly demonstrate. In the face of such complexity and controversy, there is a natural tendency to

parliamentary inaction. It is understandable. But it is dangerous. It is especially dangerous if it coincides with the disinclination of the judges (themselves often scientifically illiterate) to mobilize the creative machinery of the common law. In the field of information rights, public lethargy now conspires with unsympathetic noises both from government and opposition quarters.

Conclusions

What is the result of this analysis? Is it that late-20th-century man and woman, lulled in the global village into an intellectual haze by a constant diet of media trivia, have lost concern about political accountability? Or are they indifferent to (and even conspire in the destruction of) privacy rights? Political accountability becomes a television war between competing electoral jingles – with political parties sold like soap powder to a people programmed to watch personality politics, devoid of concern with the large issues and obsessed by the parochial. I remain incurably optimistic. But in the darker moments of contemplation, there is a lingering doubt. And even more than concern about the survival of political accountability and the persistence of privacy in the age of informatics is the institutional concern. In such a time of rapid change, of complex science and of high controversy, can our lawmaking institutions cope? That is the question that transcends even the privacy and freedom of information issues we have been gathered to discuss. They are a microcosm of a larger problem. For if our parliamentary democracies falter here, they admit their incompetence to govern us in the 21st century – whose watchword and engine will be science. Accordingly, we must remain optimistic about our capacity to adapt our institutions and laws to rapid technological change. To lose confidence or heart – and a breach of the commandment of optimism – is to surrender to the nagging doubt that technology is inherently elitist and autocratic and that democracy, with all its inefficiencies, can not survive into the 21st century. We must make it our business to ensure that this prophesy of gloom proves wrong. But the responsibility for rational optimism is ours.■

Justice Michael D Kirby, President, Court of Appeal, Supreme Court of New South Wales, Law Courts, Queen's Square, Sydney NSW 2000, Australia.

Excerpts from the keynote address to the National Forum on Access to Information and Privacy, Ottawa, Canada, March 6, 1986.

CONFERENCE ANNOUNCEMENT

WORLDCOM 86
INTERNATIONAL COMPUTER AND COMMUNICATIONS: 1986-2000

Washington DC area, USA – October 22-25, 1986

- fifty eminent speakers including ministers of PTT, heads of national telecoms, CEOs of computer and communications corporations
- video-computer teleconferences with world leaders on all continents
- exclusive meetings and receptions with senior officials of the White House, US Government, Congress and Diplomatic Corps, and bankers and investors.

The conference will be held at the International Conference Center in Reston. Further information may be obtained from Carin Christian, President, IC&C, PO Box 17392, Washington, DC 20041, USA.